UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* A One Story Home Located at 15858 San Jose Avenue, La Puente, California, as further described in Attachment A-2	Case No. 5:18-MJ-233

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-2

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-2

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 922(d)(1), (g)(1)	See attached Affidavit.

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

_____
Applicant's signature

Joseph M.G. Nazareno, ATF Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: _____

_____
Judge's signature

City and state: Riverside, California

Hon. Shashi H. Kewalramani, U.S. Magistrate Judge
Printed name and title

AUSA: Tom Rybarczyk, 213.894.8452

ATTACHMENT A-2

PREMISES TO BE SEARCHED

A house located at 15858 San Jose Avenue, La Puente, California, including all safes, lockboxes, garages, and vehicles located on the premises or under the control of the occupants of the premises ("SUBJECT PREMISES"). The SUBJECT PREMISES is a one-story, tan painted home, with a brown roof and two columns on the front porch. There are three steps leading to the front door of the SUBJECT PREMISES, which faces north in direction. Attached to the SUBJECT PREMISES is a brown wooden fence on the eastside of the SUBJECT PREMISES that can be opened to allow longer driveway access. There is a driveway on the eastside of the SUBJECT PREMISES, which leads through the wooden fence.

ATTACHMENT B-2

I. ITEMS TO BE SEIZED

1. The items to be seized are fruits, contraband, evidence, or instrumentalities of violations of Title 18, United States Code, Sections 922(d)(1) (Selling a Firearm to a Known Felon) and (g)(1) (Felon in Possession of a Firearm and Ammunition) (collectively, the "Subject Offenses"), namely:

a. Firearms and ammunition.

b. Firearms parts and accessories.

c. Tools or equipment utilized to make firearms.

d. Cash in excess of $1,000.

e. Records, documents, programs, applications, or materials, that tend to identify the person(s) in control or ownership of the SUBJECT PREMISES or a vehicle, including leases, titles, registration information, rental agreements, photographs, videos, tax documentation, driver's licenses and/or identification cards, immigration documentation, and keys, limited to 20 items.

f. Data, Records, documents, programs, applications, or materials accounting for the distribution of firearms and the remittance of firearms proceeds, including books, receipts, notes, ledgers, notebooks, computer spreadsheets, and other forms of "pay/owe" sheets.

g. Records, documents, programs, applications, or materials, listing names, aliases, telephone numbers, pager

numbers, facsimile numbers, physical addresses, and email addresses of individuals distributing firearms.

h. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show address book information, including all stored or saved telephone numbers;

i. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

j. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the trafficking firearms or transfer or laundering of the proceeds of the illegal purchase or sale of a firearm;

k. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the purchase, sale, transportation, distribution, transfer, or use of firearms;

l. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to

show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

m. Audio recordings, pictures, video recordings or still captured images related to the purchase, sale, transportation, or distribution of firearms or laundering of the proceeds of the Subject Offenses;

n. Audio recordings, pictures, video recordings or still captured images relating to firearms or ammunition;

o. Contents of any calendar or date book stored on any of the digital devices;

p. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

q. Any device used to facilitate the above-listed violations (and forensic copies thereof).

2. With respect to any digital device used to facilitate the above-listed violations containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

g. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

h. records of or information about Internet Protocol addresses used by the device; and

i. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

3. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created,

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

4. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

SEARCH PROCEDURE FOR DIGITAL DEVICES

5. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as

soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other

evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the

device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

6. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

7. During the execution of this search warrant with respect to any biometric sensor-enabled device that is located at the SUBJECT PREMISES and falls within the scope of the warrant, law enforcement personnel are authorized to: (1) depress SOLIS's thumb- and/or fingerprints onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of SOLIS's face with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

8. The special procedures relating to digital devices found in this warrant govern only the search of the SUBJECT DEVICE and/or digital devices found during the execution of the search warrant at the SUBJECT PREMISES pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Joseph M.G. Nazareno, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against and arrest warrant for ANDREW JOSE SOLIS ("SOLIS"), for a violation of Title 18, United States Code, Section 922(g)(1) (Felon in Possession of a Firearm and Ammunition). This affidavit is also made in support of an application for a warrant to search a digital device (the "SUBJECT DEVICE") seized on or about May 7, 2018 and currently in the custody of the Bureau of Alcohol, Tobacco, Firearms, and Explosives in Riverside, California, as described more fully in Attachment A-1, for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 922(d)(1) (Selling a Firearm to a Known Felon) and (g)(1) (Felon in Possession of a Firearm and Ammunition) (collectively, the "Subject Offenses"), as described further in Attachment B-1. Finally, this affidavit is made in support of an application for a warrant to search the premises located at 15858 San Jose Avenue, La Puente, California 91744 ("SUBJECT PREMISES"), as further described in Attachment A-2, to seize evidence, fruits, and instrumentalities of violations of the Subject Offenses, as further described in Attachment B-2. Attachments A-1, A-2, B-1, and B-2 are incorporated by reference.

2. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and

information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGOUND ON ATF SPECIAL AGENT JOSEPH NAZARENO

3. I am a Criminal Investigator, Special Agent ("SA") with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"), and have been so employed since January 2017. I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), and therefore, I am empowered by law to conduct investigations and make arrests for the offenses enumerated within the United States Code. I have attended the ATF Special Agent Basic Training program at the Federal Law Enforcement Training Center in Glynco, Georgia, where I received training in federal laws and regulations. I regularly refer to these laws and regulations during the course of my duties, and have participated in investigations, and the execution of search and arrest warrants for violations of these statutes. I am familiar with investigating cases involving felons in possession of firearms and am familiar with the ways in which digital devices are used to facilitate and conceal firearms transactions with individuals prohibited from possessing them.

4. Prior to working for the ATF, I was employed as a United States Probation & Pretrial Services Officer in Milwaukee, Wisconsin, for two years. In that capacity, I supervised individuals alleged to have committed, and those convicted of committing federal crimes, including offenses related to firearms, controlled substances, financial fraud, and sexually-based crimes. I also worked as a United States Probation Officer in Memphis, Tennessee, for four years, as a presentence investigator and as a supervision officer. During this time in Memphis, I also served as a certified Firearms Instructor, a Defensive Tactics Instructor, and a Search Enforcement Team Member.

5. I have received a Bachelor of Arts degree in Psychology from the University of Dallas, and a Master of Arts degree in Forensic Psychology from the Chicago School of Professional Psychology. I am currently assigned to the ATF Riverside Field Office in Riverside, California, and attached to the Riverside County District Attorney's Office Gang Impact Team in Hemet, California.

III. SUMMARY OF PROBABLE CAUSE

6. On or about May 7, 2018, officers from the West Covina Police Department ("WCPD") conducted a traffic stop on a Jeep Liberty driven by ANDREW JOSE SOLIS (the "Jeep"). SOLIS admitted that there were firearms in the Jeep and consented to a search. Officers recovered 14 firearms from the Jeep, including rifles, a shotgun, and various handguns, as well as hundreds of rounds of

live ammunition of varying calibers. At the time officers found the firearms and ammunition in the Jeep, SOLIS was a felon.

IV. STATEMENT OF PROBABLE CAUSE

7. Based on my review of law enforcement reports, my own observations, discussions with the WCPD Officers E. Melnyk and Marquez, and knowledge of this investigation, I know the following:

A. WCPD Officers See SOLIS's Vehicle Make an Illegal Right-Hand Turn and Find SOLIS in Possession of Several Firearms

8. On May 7, 2018, at approximately 9:49 p.m., WCPD Officers Melnyk and Marquez were in full-uniform and in a marked Sport Utility Vehicle ("SUV") driving northbound on Lark Ellen Avenue on their way to a service call. While driving to the service call, the officers stopped their SUV at a red light near the intersection of Lark Ellen Avenue and Rowland Avenue. Near that intersection, Lark Ellen Avenue has two lanes in either direction. The officers saw the Jeep, bearing Florida license plate number BPHW41, stopped in front of them in the number one lane of travel. The driver of the Jeep then made an illegal right-hand turn from the number one lane, in violation of California Vehicle Code Section 22100(a). At the time the Jeep's driver made the right hand turn, the Jeep was approximately 20 to 25 feet from Lark Ellen Avenue's east curb.

9. After seeing the Jeep make an illegal right turn, the officers followed the Jeep in their SUV onto Rowland Avenue and activated their overheard lights and sirens. The Jeep's driver pulled over his vehicle. Officer Marquez approached the driver

side while Officer Melnyk approached the passenger side. The driver, later identified as SOLIS, was the only person in the Jeep. As Officer Marquez spoke with SOLIS, Officer Melnyk saw a "13" tattoo on SOLIS's upper right arm that he knew, based on his training and experience, is often affiliated with La Puente 13 gang members and references loyalty to the Mexican Mafia prison gang. Officer Marquez asked SOLIS about the Florida license plate, and SOLIS said the Jeep was a rental vehicle that he obtained to drive home from Texas.

10. During the first two minutes of conversation between Officer Marquez and SOLIS, Officer Melnyk shined his flashlight in the backseat of the Jeep and saw a military-style, camouflage rifle bag, which Officer Melnyk believed, based on his training and experience, is often used to transport semi-automatic or automatic rifles. After seeing the bag, Officer Melnyk got Officer Marquez's attention and pointed at the bag. After getting Officer Marquez's attention, Officer Melnyk walked around the back to the Jeep to assist Officer Marquez with removing SOLIS from the vehicle. As Officer Melnyk walked around the Jeep, Officer Marquez asked SOLIS if the bag contained a rifle, and SOLIS said it did. Officer Marquez then asked SOLIS if he was a convicted felon and prohibited from possessing firearms. SOLIS said he was prohibited from possessing firearms because he was a felon. Officer Marquez then saw SOLIS remove his hands from the steering wheel, which prompted Officer Marquez to order SOLIS to show his hands and get out of the Jeep.

11. After SOLIS exited the Jeep, Officer Marquez asked SOLIS if he had any weapons, and SOLIS said he did not. Officer Marquez asked if they could search him, and SOLIS agreed. Officer Marquez did not find any weapons on SOLIS. Officer Marquez then asked SOLIS what was in the rifle bag, and SOLIS said, "An AR and a shotgun." Officer Marquez asked SOLIS again whether he was permitted to have possession of those weapons, and SOLIS said he was not because he was a convicted felon. Officer Marquez placed SOLIS in handcuffs and asked him if the officers could search his vehicle. SOLIS consented to the search. At this point, officers also placed SOLIS under arrest for being a felon in possession of a firearm, in violation of California Penal Code Section 29800, and possession of an assault weapon, in violation of California Penal Code Section 30605.

12. The officers proceeded to open up the rifle bag and found an unloaded AR-15 type rifle and an AR-12 shotgun inside. Officer Melnyk ran both guns serial numbers through the California Automated Firearms Systems database and learned that both guns were unregistered. While checking the front passenger area, Officer Melnyk found an empty Sig Sauer case. After Officer Melnyk told Officer Marquez this fact, Officer Marquez searched SOLIS again and found $550 in his right shorts pocket. Officer Marquez then placed him in the back of their police SUV.

13. Officer Marquez advised SOLIS of his Miranda rights and asked him about the pistol case. SOLIS told Officer Marquez he had at least three pistols in the rear part of the Jeep in a blue Adidas bag.

14. Officer Melnyk searched the SUV and located nine pistols in various bags and pistol boxes, an AK-47, and two additional AR-15 style rifles. Additionally, Officer Melynk found hundreds of rounds of ammunition.

15. In total, the officers recovered the following firearms during their search of the Jeep:

a. a TNARMS, AR-15 type pistol (serial no. A000001724);

b. a TNARMS, AR-15 type pistol (serial no. A000001717);

c. an AR-12 shotgun, Model – Magnum AR1, 12-gauge shotgun (serial no. 16-02366);

d. a Century Arms Inc., Model – RAS47, 7.62 caliber AK-47 rifle (serial no. RAS47087573);

e. an American Arms Inc., Model – Mil Sport, AR-15 pistol (serial no. MF00992);

f. a Sturm Ruger, Model – LCP, .380 caliber pistol (serial no. 372105850);

g. a Glock, Model – 19, .9mm pistol (serial no. WWU520);

h. a Smith & Wesson, Model – M&P Shield, .9mm pistol (serial no. LFB7564);

i. a Sig Sauer, Model – P938, .9mm pistol (serial no. 52B314368);

j. a Taurus International, Model – PT738, .380 caliber pistol (serial no. 02538E);

k. a Smith & Wesson, Model – SD40VE, .40 caliber pistol (serial no. HFZ7647);

l. a Smith & Wesson, Model – M&P Shield, .40 caliber pistol (serial no. HWK3752);

m. a Sturm Ruger, Model – LCP, .380 caliber pistol (serial no. 372057143); and

n. a Sig Sauer, Model – P320, .9mm pistol (serial no. 58B001541) (collectively, the "Firearms").

16. In total, the WCPD officers also found the following ammunition and magazines in the Jeep:

a. 94 live rounds of .40 caliber S&W Federal ammunition in a ZipLock bag;

b. six live rounds of .40 caliber S&W Federal ammunition in a black ammunition box;

c. 101 live rounds of .223 caliber ammunition in a black ammunition box;

d. three boxes of Federal 12-gauge shotgun shells (25 shells per box);

e. one box of Federal 12-gauge shotgun shells (10 shells per box);

f. two unloaded 7.62mm magazines;

g. two unloaded 5.56mm magazines;

h. two unloaded .40 caliber 30-round magazines;

i. one unloaded 9mm 30-round magazine;

j. one 9mm 30-round magazine prepared with 14 live rounds;

k. one unloaded 9mm 17-round magazine;

l. two unloaded 9mm 8-round magazines;

m. one 9mm 8-round magazine prepared with seven live rounds;

n. two AR-15 type magazines prepared with five live rounds;

o. one new AR-12 magazine in a box;

p. one .223 caliber drum magazine, prepared with 66 live rounds; and

q. one ammunition can containing 226 live 9mm rounds.

17. Inside the Jeep, officers also found the SUBJECT DEVICE on the driver-side front seat.[1]

18. Later, in addition to the charges described above, SOLIS was charged with committing crimes for the benefit of a street gang, in violation of California Penal Code Section 186.22, and transporting and transporting/importing assault weapons across state lines, in violation of California Penal Code Section 30600(a).

B. Law Enforcement Have Seen SOLIS at the SUBJECT PREMISES, whose Address SOLIS Has Listed as His Home Address with Probation and the California Department of Motor Vehicles

19. On or about May 7, 2018, at the time of his arrest, SOLIS told West Covina Police Officers that his address was at 16274 Appleblossom Street in La Puente, California (the "Appleblossom Address"). During the search of the Jeep, WCPD

[1] Later, while SOLIS was at the station in jail, SOLIS asked Officer Marquez to unlock the SUBJECT DEVICE and get him the number for his bail bondsmen, which Officer Marquez did.

officers found a piece of mail addressed to SOLIS at the Appleblossom Address. I queried through law enforcement databases and learned that the home associated with the Appleblossom Address is owned by Anthony and Theresa Solis, and SOLIS is listed as a possible resident of the Appleblossom Address.

20. On or about May 22, 2018 and May 25, 2018, I conducted surveillance at the Appleblossom Address and did not see SOLIS on either date.

a. After arriving at approximately 3:45 p.m. on May 22, I saw a dark blue GMC SUV, bearing California license plate number 4PIE104 (the "GMC SUV"), backing out of the driveway and departing in the opposite direction. I queried the California Department of Motor Vehicle ("DMV") database and learned that the registered owner was Anthony Solis and it was associated with the Appleblossom Address.

b. On or about May 25, 2018, I conducted surveillance again at the Appleblossom Address from approximately 5:15 a.m. to 7:45 a.m. While watching the house, I saw a Hispanic male leave the home and enter a Chevrolet pickup truck, bearing California license plate number 6F50713, parked in the driveway. I queried California DMV database and learned that the registered owners of the Chevrolet truck were Theresa and Anthony Solis and the truck was associated with the Appleblossom Address. Using California DMV database, I had obtained a photograph of Anthony Solis and compared it with the man I saw

leave the house and concluded it was the same person who drove off in the Chevrolet truck.

21. On or about May 24, 2018, I contacted the Los Angeles County Probation Department to determine the status of SOLIS's probation from his 2014 misdemeanor convictions for willful cruelty to a child, in violation of California Penal Code Section 273A, and driving under the influence, in violation of California Vehicle Code Section 23152, in the Superior Court of the State of California, County of Los Angeles, case number ELM4RI0110201. According to the probation department, SOLIS was still on probation for these offenses and the address listed for SOLIS was the SUBJECT PREMISES.

22. On the same day, May 25, 2018, I conducted surveillance at the SUBJECT PREMISES from approximately 7:50 a.m. until 8:45 a.m. During this period, I saw a man who I identified as SOLIS by comparing the man coming out from the front door of his home with SOLIS's photograph obtained from the California DMV database. After SOLIS exited the house, I saw him walk to the side of the home and return to the front of the home with a lawnmower. I then watched SOLIS mow the lawn. Later, I queried the California DMV database and learned that SOLIS provided the SUBJECT PREMISES as his home address. After querying additional law enforcement databases, I learned that Anthony Solis is the owner of the SUBJECT PREMISES, and SOLIS is listed as a possible resident of the home.

23. On May 29, 2018, I again conducted surveillance at the SUBJECT PREMISES from approximately 8:20 a.m. until 9:30 a.m. and

returned to the address from approximately 9:45 a.m. to 10:25 a.m. At approximately 9:30 a.m., I saw a woman and a child exit the SUBJECT PREMISES and appear to speak to a person inside who closed the door after the woman and child left. I saw the woman and child enter a Toyota sedan, bearing California license plate number 5ERG643. I queried the California DMV database and learned that the Toyota was registered to an Armando Solis at the SUBJECT PREMISES. After the Toyota left, I worried that I may be spotted so I drove away from the SUBJECT PREMISES for approximately 15 minutes and returned at approximately 9:45 a.m. When I returned, I saw the GMC SUV previously seen at Appleblossom Address in the driveway. As noted above, the GMC SUV is registered to Anthony Solis at the Appleblossom Address. Shortly thereafter, I saw SOLIS exit the front door of the home with an unidentified Hispanic woman. The woman got into the driver-side front seat of the GMC while SOLIS entered the passenger-side front door. I watched the GMC SUV leave the SUBJECT PREMISES.

C. SOLIS Has Prior Felony Convictions

24. On or about May 21, 2018, I reviewed SOLIS's criminal history and learned that he had the following felony convictions:

a. On or about January 21, 2009, SOLIS was convicted of Possession of a Narcotic/Controlled Substance, in violation of California Health and Safety Code Section 11350, in the Superior Court of the State of California, County of Los Angeles, in case number KA07979301; and

b. On or about February 10, 2009, SOLIS was convicted of Possession of a Controlled Substance While Armed, in violation of California Health and Safety Code Section 11370.1, in the Superior Court of the State of California, County of Los Angeles, in case number KA084719.

D. The Firearms and Ammunition Traveled in Interstate Commerce

25. On or about May 22, 2018, ATF SA Adam Rudolph, who is certified as an expert in firearms and ammunition interstate nexus, reviewed photographs of the firearms detailed above and determined that these firearms were not manufactured in State of California. Therefore, the firearms must have traveled in interstate or foreign commerce in order to have been recovered in California.

IV. TRAINING AND EXPERIENCE REGARDING FIREARMS OFFENSES

26. Based on my training, personal experience, and the collective experiences related to me by other experienced ATF special agents who specialize in firearms trafficking and firearms theft investigations, I am aware of the following:

a. People who are prohibited from owning guns but who own guns often use digital devices, including mobile phones, to coordinate buying or selling those guns, and to boast about their possession of guns to others. Such people often use calls, text messages, emails, social media, or messaging apps for these communications.

b. People who are prohibited from owning guns but who own, sell, or buy guns often use digital devices, including

mobile phones, to take photographs of the guns and of themselves with guns. They frequently send these photos to each other via text, email, social media, or messaging apps, to boast of their firearms possession.

c. People who acquire firearms illegally will often keep the information of and messages with people who supply firearms to prohibited individuals for future purchases or referrals. People who possess firearms illegally will often keep information of and messages with people to whom they may wish to sell their firearm. Many people do not dispose of their firearms-related records; they usually keep their records for long periods, often spanning several years.

d. People who possess, purchase, or sell firearms illegally generally maintain the firearms and records of their firearm transactions as items of value and usually keep them in their residence, or in places that are readily accessible, and under their physical control, such as a vehicle. Many people also keep mementos of their firearms, including digital photographs or recordings of themselves possessing or using firearms on their cell phones, smart phones, computers, and other digital devices. It has been my experience that prohibited individuals who purchase firearms illegally will keep the contact information of the individual who is supplying firearms to prohibited individuals or other individuals involved in criminal activities for future purchases or referrals. Many people do not dispose of their firearms-related records; they

usually keep their records for long periods, often spanning several years, in a secure location within their residence.

e. Individuals engaged in the illegal purchase or sale of firearms and other contraband often use multiple telephones, particularly ones with removable memory chips, known as SIM cards.

V. TRAINING AND EXPERIENCE REGARDING DIGITAL DEVICES

27. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital

devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-

spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.[2] Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the

[2] These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory

paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a

controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

28. As discussed herein, based on my training and experience I believe that digital devices will be found during the search.

a. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to

iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature

"Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

d. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

29. In my training and experience, users of electronic devices often enable the aforementioned biometric features

because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

30. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short

time. I do not know the passcodes of the devices likely to be found during the search.

31. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device.

32. For these reasons, if while executing the warrant, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to any biometric sensor-enabled device that is (a) located at the SUBJECT PREMISES and (b) falls within the scope of the warrant: (1) compel the use of SOLIS's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of SOLIS's face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

33. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

///

VII. CONCLUSION

34. For all the reasons described above, there is probable cause to believe that ANDREW JOSE SOLIS has violated Title 18, United States Code, Section 922(g)(1) (Felon in Possession of a Firearm and Ammunition). Based on the foregoing facts, there is also probable cause to believe that the items listed in Attachments B-1 and B-2, which constitute evidence, fruits, and instrumentalities of violations of the Subject Offenses described above, will be found on the SUBJECT DEVICE described in Attachment A-1 and in the SUBJECT PREMISES as described in A-2.

JOSEPH M.G. NAZARENO
Special Agent
Bureau of Alcohol, Tobacco,
Firearms, and Explosives

Subscribed to and sworn before me
this ____ day of May 2018.

HON. SHASHI H. KEWALRAMANI
UNITED STATES MAGISTRATE JUDGE